Amendments to the Specification

Please replace the paragraph that begins on Page 8, line 13 and carries over to Page 9, line 2 with the following marked-up replacement paragraph:

-- In a preferred embodiment, the 1-way function is based upon an assumption known as "the discrete logarithm with short exponent" assumption. In one aspect, the 1-way function is modular exponentiation modulo a safe prime number. In this aspect, the input value is used as an exponent of the modular exponentiation. Furthermore, a base of the modular exponentiation is a fixed generator value. Preferably, the length of the input value is 160 bits and a length of the safe prime number is 1024 bits. Alternatively, the lengths maybe greater than or equal to 160 and 1024, respectively. The length of the generated output sequence is also preferably 1024 bits, but may alternatively [[by]] be greater than 1024 bits (and in either case, is identical to the length of the safe prime number.) --

Please replace the paragraph on Page 19, lines 8 - 17 with the following marked-up replacement paragraph:

-- The rate of the PRBG in the preferred embodiment wherein C = 160 and N = 1024, generating 864 pseudo-random bits at each iteration, ~~is (864 - 160) bits~~ is 864 bits per 240 multiplications, or approximately 3.5 bits per modular multiplication. When using 20-kilobyte precomputation tables and thereby reducing the number of multiplications to 80 (as just discussed above), the rate is [[704]] 864 per 80 multiplications, or approximately [[9]] 11 bits per multiplication. With a 12-kilobyte table, according to the teachings of Lim and Lee (see "More Flexible Exponentiation with Precomputation", C. H. Lim and P. J. Lee, CRYPTO '94, LNCS

830, pp. ~~95 - 107(1994)) the~~ 95 - 107(1994)), the number of multiplications can be reduced to 40, which yields a rate of approximately 21 bits per multiplication. Using more memory, a 300-kilobyte table will yield a rate of roughly 43 pseudo-random bits per multiplication. --